Campus de la UNA
SAN LORENZO-PARAGUAY

UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

RESOLUCIÓN Nº 0732/2022

POR LA CUAL SE APRUEBA EL "MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA FP-UNA – 2022".

14 de julio de 2022

VISTO Y CONSIDERANDO: El Memorando DTIC/113/2022, de la Directora Lic. Fátima Francisca Barrios, Mg., de la Dirección de Tecnologías de Información y Comunicación de la FP-UNA, en el cual eleva la propuesta del "Manual de Políticas de Seguridad Informática FP-UNA – 2022".

La Ley N° 4995/2013 de Educación Superior.
El Estatuto de la Universidad Nacional de Asunción.

POR TANTO: en uso de sus facultades y atribuciones legales,

LA DECANA DE LA FACULTAD POLITÉCNICA
RESUELVE:

Art. 1º Aprobar el "Manual de Políticas de Seguridad Informática FP-UNA – 2022", detallados en el ANEXO de la presente Resolución.

Art. 2º Comunicar, copiar y archivar.

Lic. Vivian Antonella Fatecha Melgarejo
Secretaria de la Facultad

Prof. Ing. Silvia Teresa Leiva León, MSc.
Decana

DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN "MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA, FP-UNA 2022"

ÍNDICE

1. INTRODUCCIÓN

Con los avances en Internet y los desarrollos de la informática y las telecomunicaciones, la Seguridad Informática, se ha convertido en figura necesaria para la protección, mantenimiento, control de acceso, confidencialidad, integridad y disponibilidad de la información.

Las Políticas de Seguridad Informática (PSI) son las directrices de índole técnica y de organización que se llevan adelante respecto a un determinado sistema de computación con el fin de proteger y resguardar su funcionamiento y la información en él contenida. El principio y final de toda red es el usuario, esto hace que las políticas de seguridad deban, principalmente, enfocarse a los usuarios, indicando a las personas cómo actuar frente a los recursos informáticos de la Institución.

Actualmente la Facultad Politécnica - UNA cuenta con plataformas tecnológicas que almacenan, procesan y transmiten la información institucional e interinstitucional, incluye equipos de cómputo de usuarios y servidores que se interconectan por medio de una red de datos, así como servicio de internet, correo electrónico institucional, etc. Siendo esta información un activo valioso para la Institución, se hace necesario no solo la implementación de herramientas de hardware y software de seguridad, sino involucrar al personal para proteger su integridad y confidencialidad.

2. OBJETIVO

Definir las Políticas de Seguridad Informática que den las pautas y rijan la gestión, el uso adecuado y la seguridad de la información de los sistemas informáticos y en general, sobre el ambiente tecnológico de la Facultad Politécnica - UNA, para su interiorización, aplicación y verificación permanente, entendiendo como premisa que la responsabilidad por la seguridad de la información es de todos y cada uno.

3. ALCANCE

Las Políticas de Seguridad Informática están orientadas a toda la información almacenada, procesada y transmitida en medios electrónicos. Estas políticas deben ser conocidas y cumplidas por todos los funcionarios que apoyan la gestión y por los terceros o grupos de interés que utilicen la información generada y custodiada por la Facultad Politécnica - UNA, y por quienes hagan uso de los servicios tecnológicos de la Institución.

4. JUSTIFICACIÓN

Las Políticas de Seguridad Informática establecidas dentro de este documento son la base para la protección de los activos tecnológicos y de información de la Facultad Politécnica.

5. DEFINICIONES

Para los efectos del presente Manual, se adoptarán las siguientes definiciones:

Acceso físico: La posibilidad de acceder físicamente a una terminal, manipulándola tanto interna como externamente.

Acceso lógico: Interacción con el sistema operativo o aplicaciones, ya sea directamente, a través de la red de datos interna o de Internet.

Activo de Información: Toda aquella información que la Institución considera importante o fundamental para sus procesos, pueden ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, software del sistema, etc.

Aplicaciones o aplicativos: Son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares.

Bases de Datos: Las bases de datos son el conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.
Backup completo: se hace un respaldo completo de todos los archivos del equipo. El backup abarca el 100% de los datos.

Backup incremental: se hace una copia de todos los archivos que han sido modificados desde que fue ejecutado el último backup completo.

Cableado estructurado: Se conoce como cableado estructurado al sistema de cables, conectores, canalizaciones y dispositivos que permiten establecer una infraestructura de telecomunicaciones en un edificio. La instalación y las características de dicho sistema deben cumplir con ciertos estándares para formar parte de la condición de cableado estructurado.

Cifrado de datos: Proceso por el que una información legible se transforma mediante un algoritmo en información ilegible. Esta información ilegible se puede enviar a un destinatario con muchos menos riesgos de ser leída por terceras partes.

Configuración Lógica: conjunto de datos que determina el valor de algunas variables de un programa o de un sistema operativo, elegir entre distintas opciones con el fin de obtener un programa o sistema informático personalizado o para poder ejecutar dicho programa correctamente.

Copia de respaldo o backup: Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.

Contenido: Todos los tipos de información o datos que se divulguen a través de los diferentes servicios informáticos, entre los que se encuentran: textos, imágenes, video, diseños, software, animaciones, etc.

Contraseña: Clave utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.

Correo electrónico institucional: Es una herramienta de comunicación e intercambio de información oficial entre personas establecidas por la institución para fines institucionales.

Cuenta de acceso: Colección de información que permite a un usuario identificarse en un sistema informático o servicio, mediante un usuario y una contraseña, para que pueda obtener seguridad, acceso al sistema, administración de recursos, etc.

Dispositivos/Periféricos: Dispositivos auxiliares e independientes conectados al computador o la red.

Dominio: Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red.

Herramientas ofimáticas: Conjunto de aplicaciones informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionadas.

Información confidencial: Se trata de una propiedad de la información que pretende garantizar el acceso sólo a personas autorizadas.

Información Institucional: Entiéndase como información institucional aquella relativa a las operaciones realizadas por cada una de las dependencias de la Facultad Politécnica - UNA, su producción, almacenamiento y gestión está a cargo de cada uno de los funcionarios.

Información/Documento electrónico: Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares. Se pueden clasificar por su forma y formato en documentos ofimáticos, cartográficos, correos electrónicos, imágenes, vídeos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, entre otros.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Licencia de uso: Contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario (usuario consumidor/usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas, es decir, es un conjunto de permisos que un desarrollador le puede otorgar a un usuario en los que tiene la posibilidad de distribuir, usar y/o modificar el producto bajo una licencia determinada.

Mantenimiento lógico preventivo: Es el trabajo realizado al equipo de cómputo con la finalidad de mejorar el rendimiento general del sistema operativo y las aplicaciones.

Mantenimiento físico preventivo: El mantenimiento preventivo se entiende como un procedimiento periódico para minimizar el riesgo de fallo y asegurar la continua operación de los equipos, logrando de esta manera extender su vida útil.

Medios de almacenamiento extraíble: Son aquellos soportes de almacenamiento diseñados para ser extraídos del computador. Por ejemplo, memorias USB, discos duros externos, discos ópticos (CD, DVD), tarjetas de memoria (*SD, Compact Flash, Memory Stick).*

Plataforma web: Sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando a los usuarios la posibilidad de acceder a ellas a través de Internet.

Propiedad intelectual: Se relaciona con las creaciones de la mente como invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. Es el conjunto de derechos que corresponden a los autores y a otros titulares.

Recursos informáticos: Todos aquellos componentes de Hardware y programas (Software) que son necesarios para el buen funcionamiento de un computador o un sistema de gestión de la información. Los recursos informáticos incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.

Red de datos: Se conoce como red de datos a la infraestructura cuyo diseño posibilita la transmisión de información a través del intercambio de datos. Cada una de estas redes ha sido diseñada específicamente para satisfacer sus objetivos, con una arquitectura determinada para facilitar el intercambio de los contenidos.

Riesgo: El riesgo se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas.

Servicio informático: Conjunto de actividades asociadas al manejo automatizado de la información que satisfacen las necesidades de los usuarios.

Servidor: Un servidor es un sistema que proporciona recursos, datos, servicios o programas a otros ordenadores, conocidos como clientes, a través de una red. En teoría, se consideran servidores aquellos ordenadores que comparten recursos con máquinas cliente. Existen muchos tipos de servidores, como los servidores web, los servidores de correo y los servidores virtuales.

Sistema de información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

Software antivirus: Son programas que buscan prevenir, detectar y eliminar virus informáticos. En los últimos años, y debido a la expansión de Internet, los nuevos navegadores y el uso de ingeniería social, los antivirus han evolucionado para detectar varios tipos de software fraudulento, también conocido como malware.

Software de gestión: Son todos aquellos programas utilizados a nivel empresarial, que por su definición genera acción de emprender algo y por su aplicación persigue fines lucrativos y no lucrativos. Es un software que permite gestionar todos los procesos de un negocio o de una empresa en forma integrada. Por lo general está compuesto por módulos cruzados de los procesos del negocio.

Software malicioso: Es aquel que ha sido diseñado específicamente para dañar un computador, este tipo de software realiza acciones maliciosas como instalar software sin el consentimiento del usuario o virus.

UPS: Sistema de alimentación ininterrumpida (SAI), en inglés *uninterruptible power supply* (UPS), es un dispositivo que gracias a sus baterías y otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.

6. POLÍTICAS GENERALES DE SEGURIDAD FÍSICA

6.1. Se destinará un área en la Institución que servirá como Centro de Datos, en el cual se ubicarán los sistemas de telecomunicaciones y servidores debidamente protegidos con la infraestructura apropiada, de manera que se restrinja el acceso directo a usuarios no autorizados.

6.2. El Centro de Datos deberá contar con sistema de protección contra incendios, control de temperatura (aire acondicionado) permanente a una temperatura no superior a 22 grados centígrados, así como sistema eléctrico de respaldo (UPS).

6.3. Se deben seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.

6.4. Las instalaciones eléctricas y de comunicaciones, deberán estar preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

6.5. Se debe contar por lo menos con dos extintores de incendio adecuado y cercano al Centro de Datos.

6.6. Los equipos que hacen parte de la infraestructura tecnológica de la Facultad Politécnica - UNA, tales como servidores, estaciones de trabajo, Rack, UPS, dispositivos de almacenamiento, entre otros, deben estar protegidos y ubicados en sitios libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo.

7. POLÍTICAS ORIENTADAS A LOS USUARIOS INTERNOS

7.1. Gestión de la Información

7.1.1. Cualquier funcionario que inicie labores en la Facultad Politécnica - UNA, relacionadas con el uso de equipos de cómputo, software de gestión, aplicativos, plataformas web y servicios informáticos, debe aceptar las condiciones de confidencialidad y de uso adecuado de los recursos informáticos, así como cumplir y respetar las directrices impartidas en el Manual de Políticas de Seguridad Informática.

7.1.2. Una vez que los funcionarios se desvinculen o culminen su vínculo contractual con la Facultad Politécnica - UNA, sus accesos a los activos de la institución deberán ser revocados. También deberán hacer entrega formal de los equipos asignados, así como de la totalidad de la información electrónica que se produjo y se recibió durante el ejercicio de sus funciones.

7.1.3. Toda información recibida y producida en el ejercicio de las funciones y cumplimiento de obligaciones contractuales, que se encuentre almacenada en los equipos de cómputo, pertenece a la Facultad Politécnica - UNA, por lo tanto, no se deberá realizar divulgación ni extracción de la misma sin previa autorización de las autoridades de la Institución.

7.1.4. No se debe realizar copia no autorizada de información electrónica confidencial y software de propiedad de la Facultad Politécnica - UNA. El retiro de información electrónica perteneciente a la Facultad Politécnica - UNA y clasificada como confidencial, se hará única y exclusivamente con la autorización del Directivo competente.

7.1.5. Ningún funcionario deberá visualizar, copiar, alterar o borrar información para la cual no se encuentre autorizado.

7.1.6. Todo contrato o convenio relacionado con servicios de tecnología y/o acceso a información, debe contener una obligación o cláusula donde el contratista o tercero acepte el conocimiento de las políticas de seguridad y acuerde mantener confidencialidad de la información con la suscripción de un acuerdo o compromiso de confidencialidad de la información, el cual se hará extensivo a todos sus colaboradores.

7.2. Hardware y Software

7.2.1. La instalación y desinstalación de software, la configuración lógica, conexión a red, instalación y desinstalación de dispositivos, la manipulación interna y reubicación de equipos de cómputo y periféricos, deberá ser realizada únicamente por personal del área de la Dirección de Tecnologías de Información y Comunicación (en adelante DTIC).

7.2.2. El espacio en disco duro de los equipos de cómputo pertenecientes a la Facultad Politécnica - UNA debe ser ocupado únicamente con información institucional, no se debe hacer uso de ellos para almacenar información de tipo personal (documentos, imágenes, música, video, etc.).

7.2.3. Ningún funcionario debe acceder a equipos de cómputo diferentes al suyo sin el consentimiento explícito de la persona responsable de dicho equipo.

7.2.4. Ningún funcionario deberá acceder o interceptar datos informáticos en su origen, destino o en tránsito, protegido o no con una medida de seguridad, sin autorización.

7.2.5. Ningún funcionario deberá impedir u obstaculizar el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos o a una red de telecomunicaciones, salvo el personal autorizado del área de TIC en aplicación de las políticas o medidas de seguridad.

7.2.6. No se permite el uso de la plataforma y servicios informáticos (equipos de cómputo, periféricos, dispositivos, Internet, red de datos, correo electrónico institucional) de la Facultad Politécnica - UNA, para actividades que no estén relacionadas con las labores propias de la Institución.

Los funcionarios serán responsables de contar con conocimientos actualizados en informática básica y el uso de herramientas ofimáticas

7.3. Correo Electrónico

7.3.1. La solicitud de la cuenta de correo deberá ser solicitada a DTIC por los canales correspondientes establecidos, mencionando los motivos por los que se solicita el servicio, el nombre completo, número de cédula de identidad, departamento al cual corresponde, correo alternativo (no institucional) y un número de teléfono personal para contactos en casos de necesidad. Finalizada la vinculación del usuario con la FP-UNA, las cuentas de correo podrán ser eliminadas en caso de no ser necesaria la información allí contenida.

7.3.2. Los funcionarios no deben utilizar cuentas de correo asignadas a otras personas.

7.3.3. El correo electrónico institucional es exclusivo para envío y recepción de datos relacionados con las actividades de la Facultad Politécnica - UNA, no se hará uso de él para fines personales como registros en redes sociales, registros en sitios Web con actividades particulares o comerciales, o en general para comunicaciones de asuntos no relacionados con las funciones y actividades en la Institución.

7.3.4. La información transmitida a través de las cuentas de correo electrónico institucional no se considera correspondencia privada, ya que éstas tienen como fin primordial la transmisión de información relacionada con las actividades ordinarias de la institución. La FP-UNA podrá auditar el contenido de los mensajes en casos de controversias o incumplimiento de los términos, acuerdos o normas vigentes.

7.3.5. Los mensajes de correo electrónico y archivos adjuntos, deben ser tratados como información privada de la institución.

7.3.6. Está prohibido utilizar el correo electrónico institucional para divulgar información confidencial, reenviar mensajes que falten al respeto o atenten contra la dignidad e intimidad de las personas, difundir propaganda política, comercial, religiosa, racista, sexista o similares, reenviar contenido y anexos que atenten contra la propiedad intelectual.

7.3.7. Está prohibido interceptar o revelar comunicaciones electrónicas, ni ayudar a terceros a realizarlo.

7.3.8. Es responsabilidad del funcionario depurar su cuenta de correo periódicamente, en todo caso debe hacer copia de seguridad completa de los correos tanto recibidos como enviados.

7.4. Internet

7.4.1. La asignación de servicio de Internet deberá ser solicitada a DTIC por los canales correspondientes establecidos.

7.4.2. El Servicio de Internet de la Facultad Politécnica - UNA no deberá ser usado para fines diferentes a los requeridos en el desarrollo de las actividades propias de la Institución. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás, cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

7.4.3. No se debe descargar archivos vía Internet que no provengan de páginas conocidas o relacionadas con las funciones y actividades en la Institución.

7.4.4. No está permitido el uso de Internet para actividades ilegales o que atenten contra la ética y la imagen de la Facultad Politécnica - UNA o de las personas.

7.4.5. La Facultad Politécnica - UNA se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet de la Institución.

7.4.6. Los usuarios deben reportar todos los incidentes de seguridad detectados a DTIC, a través de los canales correspondientes establecidos para el caso.

7.5. Cuentas de Acceso:

7.5.1. Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información deberán ser solicitadas a la Dirección de DTIC por los canales correspondientes establecidos, mencionando los motivos por los que se solicita el servicio, indicando nombre completo del funcionario, número de documento, correo electrónico institucional y dependencia a la que pertenece.

7.5.2. Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles, cada funcionario es responsable por las cuentas de acceso asignadas y las transacciones que con ellas se realicen. Se permite su uso única y exclusivamente durante el tiempo que tenga vínculo laboral o contractual con la Facultad Politécnica - UNA.

7.5.3. Las contraseñas de acceso deben poseer un mínimo de ocho (8) caracteres y debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (+-*/@#$%&). No debe contener vocales tildadas, ni eñes, ni espacios. Por seguridad, las contraseñas no deben contener fechas, nombres, o cualquier dato que lo vincule con el usuario.

7.5.4. La contraseña inicial de acceso a la red que le sea asignada debe ser cambiada la primera vez que acceda al sistema, además, debe ser cambiada al menos una vez cada 6 meses, o cuando se considere necesario debido a alguna vulnerabilidad en los criterios de seguridad.

7.5.5. Solamente puede solicitar cambio o restablecimiento de contraseña, el funcionario al cual pertenece dicho usuario, o el jefe inmediato mediante solicitud enviada por correo electrónico a DTIC.

7.5.6. Todo funcionario que se retire de la Institución de forma definitiva o temporal (superior a 1 semana), deberá hacer entrega (si es necesario) formal, a quien lo reemplace en sus funciones o a su superior inmediato, de las claves de acceso de las cuentas asignadas, con el fin de garantizar la continuidad de las operaciones a su cargo.

7.6. Seguridad Física:

7.6.1. Es responsabilidad de los funcionarios velar por la conservación física de los equipos a ellos asignados, haciendo uso adecuado de ellos. En el caso de equipos que deban ser retirados para brindar servicios externos, estos podrán ser retirados de las instalaciones de la Institución única y exclusivamente por el usuario a cargo y estrictamente para ejercer labores que estén relacionadas con la Facultad Politécnica - UNA, previa autorización de su Director. En caso de daño, pérdida o robo, se establecerá su responsabilidad a través de los procedimientos definidos por la normatividad para tal fin.

7.6.2. Los funcionarios deberán reportar de forma inmediata a DTIC la detección de riesgos reales o potenciales sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes, peligro de incendio, peligro de robo, entre otros. Así como reportar de algún problema o violación de la seguridad de la información, del cual fueren testigos.

7.6.3. Mientras se utilicen los equipos de cómputo, no se deberán consumir alimentos ni ingerir bebidas sobre el mismo escritorio.

7.6.4. Se debe evitar colocar objetos encima de los equipos de cómputo que obstruyan las salidas de ventilación del monitor o de la CPU.

7.6.5. Se debe mantener el equipo de cómputo en un lugar limpio y libre de humedad.

7.6.6. Se debe evitar colocar objetos encima o contra los cables de conexión.

7.6.7. Solo el personal autorizado puede realizar mantenimiento o reparación del equipo de cómputo, por lo tanto, el mismo sólo puede ser abierto o desarmado por personal autorizado.

7.6.8. Es responsabilidad de los funcionarios que utilicen el equipo asegurarse de respaldar la información que consideren relevante cuando el equipo vaya a reparación, ya que de acuerdo al inconveniente que presente el equipo, la información contenida podría no ser recuperada, por lo que es responsabilidad del usuario mantener copias de respaldo de la información.

7.6.9. El funcionario deberá de dar aviso inmediatamente a las autoridades correspondientes en caso de desaparición, robo o extravío del equipo de cómputo o accesorios que se tenga bajo su resguardo.

7.7. Derechos de Autor

7.7.1. Está prohibido realizar copias no autorizadas de software, ya sea adquirido o desarrollado por la Institución.

7.7.2. Los sistemas desarrollados por personal interno y externo, son propiedad intelectual de la Facultad Politécnica – UNA.

7.7.3. Ningún usuario debe descargar y/o utilizar información, archivos, imagen, sonido, software u otros que estén protegidos por derechos de autor de terceros sin la previa autorización de los mismos.

7.8. Uso de Unidades de Almacenamiento Extraíbles

7.8.1. Los funcionarios que tengan información de propiedad de la Facultad Politécnica - UNA en medios de almacenamiento removibles deben proteger el acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

7.8.2. Toda información que provenga de un archivo externo de la Institución o que deba ser restaurado tiene que ser analizado con el antivirus institucional vigente.

7.9. Clasificación de la información

7.9.1. Los documentos electrónicos resultantes de los procesos misionales y de apoyo de la Facultad Politécnica - UNA, se tratarán conforme a los lineamientos y parámetros establecidos en el Sistema de Gestión Documental de la institución. Los activos de información asociados a cada sistema de información serán identificados y clasificados por su tipo y uso siguiendo lo establecido en las tablas de retención documental vigentes.

7.10. Personal de DTIC

7.10.1. El control de los equipos tecnológicos deberá estar bajo la responsabilidad de DTIC, así como la asignación de usuarios y la ubicación física.

7.10.2 DTIC deberá llevar un control total y sistematizado de los recursos tecnológicos tanto de hardware como de software.

7.10.3. DTIC será la encargada de velar por que se cumpla con la normatividad vigente sobre propiedad intelectual de soporte lógico (software).

7.10.4. Las licencias de uso de software estarán bajo custodia de DTIC. Así mismo, los manuales y los medios de almacenamiento (CD, pen drive u otros medios) que acompañen a las versiones originales de software.

7.10.5. DTIC es la única dependencia autorizada para realizar copia de seguridad del software original, aplicando los respectivos controles. Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

7.10.6. Todas las publicaciones que se realicen en el sitio WEB de la Institución deberán atender el cumplimiento de las normas en materia de propiedad intelectual.

7.10.7. Se deben asignar usuarios unificados para todos y cada uno de los sistemas, servicios y aplicaciones, garantizando la estandarización por cada usuario; es decir, que cada usuario debe tener el mismo nombre de usuario para todos los sistemas y aplicaciones de la Institución. La estandarización de los nombres de usuario estará compuesta de la siguiente forma: Primera letra del primer nombre + primer apellido; en caso de existir duplicidad, Primeras dos letras del primer nombre + primer apellido.

7.10.8. Las cuentas de acceso a sistemas, servicios y aplicaciones no podrán ser eliminadas al momento de la desvinculación del funcionario, debe aplicarse la inactivación del usuario.

7.10.9. Se realizará backup a la información institucional y bases de datos, conforme a lo establecido en la política de backup y cronograma, así como en los casos extraordinarios: desvinculación del funcionario, envío de equipo para garantía, mantenimiento correctivo de equipo.

7.10.10. Las contraseñas de los usuarios administradores de las plataformas tecnológicas y sistemas de información de la Institución deberán ser salvaguardadas por DTIC en un archivo protegido a través de técnicas de cifrado de datos u otro mecanismo seguro.

7.10.11. La red interna de la Facultad Politécnica - UNA deberá estar protegida de amenazas externas, a través de sistemas que permitan implementar reglas de control de tráfico desde y hacia la red.

7.10.12. Todos los equipos de la institución deben tener instalado un antivirus, en funcionamiento y actualizado.

7.10.13. Se debe realizar mantenimiento lógico preventivo a los equipos de cómputo, mínimo una vez por año, que incluya el cableado estructurado. DTIC deberá elaborar el plan y cronograma de mantenimientos, el cual será notificado a los usuarios, adicionalmente, deberá informarse el nombre e identificación del personal autorizado para realizar las actividades de mantenimiento con el fin de evitar el riesgo de hurto y/o pérdida de equipos e información.

7.11. Directivos

7.11.1. La Institución deberá garantizar capacitación a los funcionarios en el manejo del software de gestión, plataformas y aplicativos implementados en la Facultad Politécnica - UNA.

7.11.2. Se deberá notificar a DTIC las novedades de vinculación y desvinculación de personal de la Facultad Politécnica - UNA, así como también del movimiento entre dependencias de un funcionario, con el fin de crear modificar o cancelar, según sea el caso, los accesos a los sistemas de información, correo electrónico y red de datos.

8. POLÍTICAS ORIENTADAS A LOS USUARIOS EXTERNOS

8.1. El acceso de terceras personas a la Institución debe ser controlado y su ingreso a las diferentes dependencias debe ser autorizado por los funcionarios a cargo.

9. POLÍTICA DE ADMINISTRACIÓN DE BACKUP

9.1. Las informaciones institucionales deben ser respaldadas por lo menos una vez por semana.

9.2. Las copias de seguridad deben ser almacenadas en un Disco Duro extraíble dispuesto exclusivamente para este fin, en equipos específicos de backup o en la nube.
9.3. Cada copia de seguridad realizada debe ser registrada de tal forma que se pueda restaurar la información de una fecha determinada en caso de necesidad.

9.4. Las copias de seguridad se deben realizar bajo el método de backup completo y backup incremental.

9.5. La copia de respaldo de base de datos debe realizarse todos los días de forma automática y debe mantenerse por lo menos durante 7 días de forma local.

9.6. La copia de respaldo de base de datos debe realizarse todos los días de forma automática y debe mantenerse por lo menos durante 1 mes en equipos de backup dentro de la institución, fuera del Centro de Datos.

9.7. La copia de respaldo de base de datos debe realizarse por lo menos una vez al mes en la nube.

10. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL SITIO WEB

El sitio web de la Facultad Politécnica - UNA (FP-UNA) tiene como función principal proveer información y servicios, así como divulgar y promover normas y directrices internas y del Gobierno Nacional relacionadas con su objeto.

Conforme a los lineamientos de la Estrategia de Gobierno en Línea, la FP-UNA pública los temas y actividades que tienen que ver con su misión, visión, objetivos y funciones por medio de su página www.pol.una.py, informando sobre: trámites, servicios, indicadores de gestión, planes y programas, publicaciones, normas, convocatorias, información presupuestal, enlaces institucionales, etc.

10.1. Aceptación de Términos

10.1.1. Se presume que cuando un usuario accede al sitio web de la FP-UNA lo hace bajo su total responsabilidad y que, por tanto, acepta plenamente y sin reservas el contenido de los siguientes términos y condiciones de uso del sitio web de la institución.

10.1.2. Esta declaración de uso adecuado de la información está sujeta a los términos y condiciones de la página web de la FP-UNA, con lo cual constituye un acuerdo legal entre el usuario y la página de la FP-UNA.

10.1.3. Si el usuario utiliza los servicios de la página web de la FP-UNA, significa que ha leído, entendido y aceptado los términos expuestos. Si no está de acuerdo con ellos, tiene la opción de no proporcionar ninguna información personal, o no utilizar el servicio de la página web de la FP-UNA, www.pol.una.py.

10.2. Condiciones generales respecto al contenido del sitio web

10.2.1. La FP-UNA se reserva, en todos los sentidos, el derecho de actualizar y modificar en cualquier momento y de cualquier forma, de manera unilateral y sin previo aviso, las presentes condiciones de uso y los contenidos de la página Web www.pol.una.py.

10.2.2. El sitio Web tiene por finalidad brindar al usuario todo tipo de información relacionada con la gestión de la Facultad Politécnica - UNA. La información contenida en esta página Web, debe estar redactada de forma breve, sencilla y clara.

10.2.3. El sitio Web puede tener enlaces a otros sitios de interés o documentos localizados en otras páginas Web de propiedad de otras entidades, personas u organizaciones diferentes a la FP-UNA. En estos casos el usuario deberá someterse a las condiciones de uso y a la política de privacidad de las respectivas páginas Web.

10.2.4. La FP-UNA no se hace responsable respecto a la información que se halle fuera de este sitio Web y no sea gestionada directamente por el administrador del sitio Web www.pol.una.py.

10.2.5. Los vínculos (links) que aparecen en el sitio Web tienen como propósito informar al usuario sobre la existencia de otras fuentes susceptibles de ampliar los contenidos que ofrece la página Web o que guardan relación con ellos.

10.2.6. La FP-UNA no garantiza ni se responsabiliza del funcionamiento o accesibilidad de las páginas Web vinculadas. Tampoco sugiere, invita o recomienda la visita a las mismas. Por eso, no será responsable del resultado obtenido.

10.2.7. El establecimiento de un vínculo (link) con el sitio Web de otra empresa, institución o programa no implica necesariamente la existencia de relaciones entre la FPUNA y el propietario del sitio o página Web vinculada, ni la aceptación o aprobación por parte de la FP-UNA de sus contenidos o servicios.

10.2.8. Las personas que usen el vínculo (link) de la página de la FP-UNA, deberán abstenerse de realizar manifestaciones o indicaciones falsas, inexactas o incorrectas sobre la FP-UNA o incluir contenidos ilícitos, o contrarios a las buenas costumbres y al orden público.

10.2.9. Las investigaciones publicadas en la página Web de la FP-UNA no implican, de parte de la Entidad, juicio alguno o comprometen la posición de la institución y/o de quienes intervienen en ella. Los contenidos son responsabilidad de quienes realizaron la investigación.

10.2.10. La prestación del servicio del sitio Web de la FP-UNA es de carácter libre y gratuito para los usuarios y se rige por los términos y condiciones que aquí se incluyen, los cuales se entienden como conocidos y aceptados por los usuarios del sitio.

10.3. Derechos de autor de los contenidos de la página Web - Copyright

Este sitio de Internet y su contenido son de propiedad intelectual de la FP-UNA. Es posible descargar material de www.pol.una.py para uso personal y no comercial, siempre y cuando se haga expresa mención de la propiedad de la FP-UNA.

Respecto a los contenidos que aparecen en el sitio Web de la FP-UNA, el usuario se obliga a:

a. Usar los contenidos de forma diligente, lícita y correcta.

b. No suprimir, eludir, o manipular el copyright (derechos de autor) y demás datos que identifican los derechos de la FP-UNA.

c. No emplear los contenidos y en particular la información de cualquier otra clase obtenida a través de la FP-UNA o de los servicios, para emitir publicidad.

d. La FP-UNA no será responsable por el uso indebido que hagan los usuarios del contenido de su sitio Web.

e. El visitante o usuario del sitio Web se hará responsable por cualquier uso indebido, ilícito o anormal que haga de los contenidos, información o servicios del sitio de la FP-UNA. El visitante o usuario del sitio, directa o por interpuesta persona, no debe atentar de ninguna manera contra el sitio Web de la FP-UNA, contra su plataforma tecnológica, contra sus sistemas de información ni tampoco debe interferir en su normal funcionamiento.

f. El visitante o el usuario del sitio no debe alterar, bloquear o realizar cualquier otro acto que impida mostrar o acceder a cualquier contenido, información o servicios del sitio Web de la FP-UNA, o que estén incorporados en las páginas Web vinculadas.

g. El visitante o el usuario del sitio Web de la FP-UNA no debe enviar o transmitir en este sitio o hacia el mismo a otros usuarios o a cualquier persona cualquier información de alcance obsceno, difamatorio, injuriante, calumniante o discriminatorio.

h. El visitante o el usuario del sitio Web de la FP-UNA no debe incurrir en conductas ilícitas, como daños o ataques informáticos, interceptación de comunicaciones, infracciones a los derechos de autor, uso no autorizado de terminales, usurpación de identidad, revelación de secretos o falsedad en los documentos.

10.4. Ley Aplicable y Jurisdicción

10.4.1. El usuario no podrá manifestar ante la FP-UNA o ante una autoridad judicial o administrativa, la aplicación de condición, norma o convenio que no esté expresamente incorporado en las presentes condiciones de uso.

10.4.2. Estas condiciones serán gobernadas por las leyes de la República de Paraguay, en los aspectos que no estén expresamente regulados en ellas.

10.4.3. Si cualquier disposición de estas condiciones pierde validez o fuerza obligatoria, por cualquier razón, todas las demás disposiciones, conservan su fuerza obligatoria, carácter vinculante y generarán todos sus efectos.

10.4.5. Para cualquier efecto legal o judicial, el lugar de las presentes condiciones es el Municipio de San Lorenzo, Departamento Central, República de Paraguay, y cualquier controversia que surja de su interpretación o aplicación se someterá a los jueces de la República de Paraguay.

10.5. Duración y terminación

10.5.1. La prestación del servicio del sitio WEB de la FP-UNA tiene una duración indefinida. Sin embargo, la entidad podrá dar por terminada o suspender la prestación de este servicio en cualquier momento. En caso de que se llegue a presentar esta situación, la FP-UNA informará previamente sobre el hecho.

11. CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

11.1.1. Los directores, coordinadores y DTIC, son responsables de conocer y asegurar la implementación de las políticas de seguridad informática, dentro de sus áreas de responsabilidad, así como del cumplimiento de las políticas por parte de su equipo de trabajo. El no cumplimiento de las Políticas de Seguridad Informática conllevará a sanciones administrativas y legales pertinentes.